Monitoring with Graylog

A modern approach to monitoring?

Christoph Petrausch
Karlsruhe, 06.11.2015
Christoph Petrausch
Systems Engineer @ inovex GmbH

› Platform Engineering
› System Automation & Development (DevOps)

› Blog, Slides & Videos at inovex.de
Agenda

1. Why Graylog?
2. What is Graylog?
3. Demo
4. Conclusions
5. Q&A
Why Graylog?

Existing monitoring solutions (Nagios, Icinga, Zabbix) have problems:

- Some of them lack of APIs
- Integration with configuration management is very time-consuming
- Do not scale well
- High Availability is not considered by the System Architecture
Project Overview

- Open Source Project, GPLv3
- Project started in 2009
- Company Graylog Inc. is the main developer
- Around a dozen contributors on GitHub
What does Graylog?

› Receives messages from multiple input protocols
  › GELF via HTTP/UDP/TCP, Syslog, Apache Kafka, ….
› Assigns messages to streams
› Triggers user-defined alerts per stream
› Stores messages in ElasticSearch for graphing
› Routes messages to different outputs based on streams
› Provides search and graphing capabilities for stored messages
› Uses MongoDB to store metadata and alerts
GELF (Graylog Extended Log Format)

› Compressed or uncompressed JSON string
› JSON Hash with mandatory fields:
   › host, version, short_message, full_message, timestamp, level
› Additional custom fields start with an underscore
Architecture

http://docs.graylog.org/en/1.2/pages/architecture.html#bigger-production-setup
Message Processing
Plugins

- Are written in Java
- Nearly all parts of Graylog are extensible
  - Inputs
  - Outputs
  - Services
  - Alarm callbacks
  - Filters
  - REST API resources
  - Periodical tasks
Hands on: Demo
Conclusion

› Only one index for all messages
  › Same named fields have to have the same semantics
› Rudimentary graphs
  › No interactive zooming
› Rudimentary alarming configuration
› High configuration effort to get “per-host” monitoring
  › But you can do it via a REST-API!
Q&A
Thank You!

Christoph Petrausch
IT Engineering & Operations

inovex GmbH
Ludwig-Erhard-Allee 6
76131 Karlsruhe (GER)

christoph.petrausch@inovex.de